SANDIA REPORT
SAND2003-8398
Unlimited Release
Printed July 2003

Position Paper on Active Countermeasures for Computer Networks

Jamie A. Van Randwyk

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2003-8398
Unlimited Release
Printed July 2003

Position Paper on Active Countermeasures for Computer Networks

Jamie A. Van Randwyk
Information Security
Sandia National Laboratories
PO Box 969
Livermore, CA 94551-9011

Abstract

Computer security professionals have used passive network countermeasures for several years in order to secure computer networks. Passive countermeasures such as firewalls and intrusion detection systems are effective but their use alone is not enough to protect a network. Active countermeasures offer new ways of protecting a computer network. Corporations and government entities should adopt active network countermeasures as a means of protecting their computer networks.

Introduction

Providing security to computers on networks is a relatively new art, though the techniques used to do so have roots in defensive measures used by the military for centuries. The military has relied on many different types of countermeasures to aid in conflict, most of which can be categorized as passive or active.

Passive countermeasures have been the traditional devices used in providing network security. The development of security techniques has slowed, maybe even stalled, in recent years. While vendors are adding new (and sometimes useful) features to firewalls and Intrusion Detection Systems (IDSs), the rate of computer break-ins continues to increase. The problem with the current network security paradigm is that passive countermeasures have not stopped or slowed security compromises.

Information security professionals, system administrators, and managers of these people need to look at active countermeasures in order to respond to network attacks. As defined by [1], a countermeasure is "an action or device designed to negate or offset another." In my research an **active network countermeasure** is defined as *a countermeasure that sends network traffic to the perceived source that produced the offending behavior.*

Passive Countermeasures

The above definition is in contrast to passive network countermeasures such as firewalls, software patches, and intrusion detection that do not directly respond to the perceived source of an attack. Described below are a few passive countermeasures and why they are useful but lacking necessary characteristics for defending a computer network.

The first and maybe most popular of these passive countermeasures is the firewall. Firewalls fulfill the role for which they were designed, but holes still exist even when a firewall is configured properly in a network. This is illustrated by firewall rules that are written so certain incoming ports are open to the world either for convenience sake or to allow for ease of use for the users behind the firewall. An example of this is active mode FTP where port 20 is typically opened to allow an inbound data connection in concert with an outbound control connection. This allows for port scans and vulnerability exploitation of machines behind the firewall provided that these actions are initiated from source port 20. More recently, firewalls have been promoted as the only tool necessary for securing a computer or network. This is most easily seen by the current practice of marketing personal firewalls as the ultimate security solution.

Applying software patches is another of the common passive countermeasures. This has become a full-time job at some large organizations. Most IT professionals realize that software patches are only a temporary countermeasure to poorly coded software though. Software patches will not suffice as adequate countermeasures even with remote software distribution systems such at netOctopus. Using software patches as a countermeasure will fail at many small organizations because these organizations often lack the size to hire dedicated IT staff. Large organizations will not be protected by the software patch countermeasure because some computers will inevitably fall through the cracks. In addition, the turnaround time from disclosure of a vulnerability to distribution of a patch on a corporate network can often be too long. Full disclosure of software vulnerabilities is now closely followed by distribution of proof-of-concept code that exploits those vulnerabilities which is then followed itself by distribution of malicious code that incorporates the proof-of-concept code.

Intrusion detection systems are used as another type of passive countermeasure. They have created a buzz in the academic and corporate worlds as the latest and greatest network security systems. IDSs are well tuned to alert system administrators and security personnel to possible break-ins. Some IDSs even trigger automatic blocking of source IP addresses using Access Control

Lists (ACLs). IDSs do miss intrusions and remote scans though. Slow network scans are hard to detect using IDSs. Sometimes network attacks come days or even months after the initial reconnaissance done by the attacker. Most IDSs on the market do not issue intrusion alerts in real time. If they do, security administrators are usually so overwhelmed with alerts that they cannot respond in real time.

Active network countermeasures

Active network countermeasures provide many new lines of defense in network security. They can be used to "fill" empty address space. Despite the available IPv4 address space being reported as rapidly dwindling, many organizations own large blocks of address space that are actually populated very sparsely. This makes target hosts easy to find for a would-be attacker using widely available network reconnaissance tools such as *nmap*. A simple network response program can be written so that the network appears to be fully populated to those tools. Our experience has shown that a simple measure such as this is enough to convince a would-be attacker to move his/her scanning and attacking on to a different network.

The second feature active countermeasures provide is to hold an attacker in a honeypot, whether a physical or virtual honeypot. Tools such as *honeyd* by Niels Provos (found at [2]) can be used to fill the empty address space with virtual computers or even virtual networks. Attackers use fingerprinting tools to determine the operating system being run on possible target machines. The results of these fingerprint scans give an attacker a good idea as to which machines he/she wants to attack based on potential vulnerabilities. Virtual honeypot hosts can be made to look like computers running any imaginable operating system with a wide array of user programmable services running on those hosts. The *honeyd* tool is customizable to the point that an attacker would have a hard time determining whether a physical computer exists at a given IP address rather than a virtual host.

Using a honeypot as a countermeasure fulfills a different goal than the usual use of physical honeypots. The purpose is not to study the behavior of attackers as is typically done, but rather the purpose is to trap, distract, and confuse attackers. Physical and virtual honeypots alike can offer enough feedback to an attacker to cause him/her to spend a lot of time in the honeypot. This sort of countermeasure succeeds by containing/trapping the attacker in an area where he/she is not interfering with business-critical computing. Honeypots serve to keep attackers away from business-critical machines by appearing more attractive to attackers than the surrounding authentic hosts on authentic networks. Honeypots achieve this goal by carefully choosing banner strings to return in response to network service probes. For instance, when an attacker scans a network for vulnerable versions of an FTP server as reported by the server's banner string, a honeypot machine (physical or virtual) can send back a vulnerable server string in order to attract the attacker.

The third countermeasure feature provided by honeypots is the ability to confuse and frustrate attackers. A network set up as described in the first active countermeasure example above will cause a Class B or CIDR /16 network to appear to have over 65,000 active hosts when probed by an attacker. Just as a network with completely filled address space will confound an attacker and cause him/her to move on to a different network, a network with confusing or unbelievable characteristics will do the same. Virtual hosts can be configured to respond to network OS fingerprint scans as any conceivable OS with a TCP/IP network stack. Configuring a network to appear to have 5,000 high-powered Cisco routers or 3,000 FreeBSD 2.0 machines could convince an attacker to move on to more susceptible networks. Beyond simple emulation of a host on a network, the network itself can be virtualized. Causing a given network of any size to suffer from a terrible packet loss problem only when communicating with even numbered IP addresses could likewise cause an attacker to

rethink his/her selection method for choosing victim networks.

Active network countermeasures not only provide immediate security by trapping or confusing an attacker, but active countermeasures can also indirectly aid in network security research. This is similar to the purpose of physical honeypots where compromised systems reveal valuable information describing the current threat. With strategically coded virtual honeynets virus and worm data can be collected without infecting physical machines. Responding in certain ways to viruses or worms will trigger the attacking code to send information and sometimes itself to the supposed target. A system administrator can then analyze the executable or even source code of the virus/worm. The system administrator can then make changes to existing passive and active countermeasures to defend against the virus and/or worm.

In addition to capturing worm and virus data for analysis, active countermeasures can be used to contain a worm and keep it from spreading. Responding to a worm in a certain prescribed manner can cause the worm to become trapped while trying to infect a network, keeping it from moving on to new targets.

Additional issues in using active countermeasures

When using active network countermeasures, care should be taken so as not to impair legitimate/sanctioned use of the network. RFC791 states a general rule of thumb to apply when implementing the Internet Protocol: "An implementation must be conservative in its sending behavior, and liberal in its receiving behavior." This principle should apply when actively responding to network traffic so that legitimate traffic is not mistook for hostile traffic. The degree to which this applies, of course, depends on the nature of the network being protected and, therefore, is a matter of policy within the protected organization.

A person employing active countermeasures on their network must also be aware of the legal issues involved with doing such. Active countermeasures could be implemented in such a way that a system administrator breaks the law when trying to defend his/her network from someone who is breaking the law.

Summary

Traditional security methods including passive countermeasures are not complete solutions when securing networks and hosts on those networks. Though their use has provided many a system administrator with timely protection, they lack the dynamic interaction that appears to be critical when defending a network. Blocking network datagrams via a firewall provides security at the cost of usability. Plugging security holes is an essential system administration task, but patch distribution is an evolving art. While detecting attacks and sending alerts with IDSs has come a long way, current rule-based systems miss some of attacks.

Active countermeasures offer a new way of protecting a network. They provide security by participating in the typical commerce seen on a network. Active countermeasures fill address space, trap and frustrate attackers, and contribute to stopping viruses and worms. These countermeasures do not simply report or block attacks, but they attempt to deceive the attacker by presenting a network in the best way possible to deter such actions.

Academia and industry need to look beyond the current network security paradigm to the innovative solutions that active countermeasures can offer. Continued support for research in developing new active countermeasures and refining existing ones should be pursued by government agencies and industry. Small-scale deployment and testing of active countermeasures is needed at both the corporate and government levels now, while larger scale implementations should be planned soon. Advances in computer network attacks demand smarter defense mechanisms to combat smarter attackers. We must raise the bar if we are to

protect our assets and keep the attacker at bay.

Acknowledgements

I would like to thank James Hutchins for sharing his background in countermeasure research and providing relevant examples. Eric Thomas provided much help in the way of code and new ideas. Timothy Toole offered his insight into legal issues surrounding the use of active network countermeasures. Finally, I would like to thank Niels Provos for his excellent active countermeasure tool, *honeyd,* and for allowing us to contribute to its development and integrate it into our own work.

References

[1] http://www.m-w.com, December 2002.
[2] honeyd.
http://www.citi.umich.edu/u/provos/honeyd/
.

Distribution

1	MS 0455	R. S. Tamashiro
1	MS 0630	D. H. Schroeder
1	MS 0801	A. L. Hale
1	MS 0801	W. F. Mason
1	MS 0801	M. R. Sjulin
1	MS 0806	J. A. Hudson
1	MS 0806	P. C. Jones
1	MS 0806	M. M. Miller
1	MS 0806	L. Stans
1	MS 0812	R. L. Adams
1	MS 0813	R. M. Cahoon
1	MS 0813	S. R. Carpenter
1	MS 0813	D. M. Kayatt Jr.
1	MS 0813	A. A. Quintana
1	MS 0813	R. A. Suppona
1	MS 9003	P. W. Dean
1	MS 9003	C. M. Hartwig
1	MS 9003	K. E. Washington
1	MS 9011	N. A. Durgin
1	MS 9011	B. V. Hess
1	MS 9011	J. D. Howard
1	MS 9011	S. A. Hurd
1	MS 9011	J. A. Hutchins
1	MS 9011	E. D. Thomas
1	MS 9011	T. J. Toole
5	MS 9011	J. A. Van Randwyk
1	MS 9012	J. A. Friesen
1	MS 9012	S. C. Gray
1	MS 9012	P. E. Nielan
1	MS 9019	S. C. Carpenter
1	MS 9019	B. A. Maxwell
1	MS 9037	J. C. Berry
1	MS 9217	S. W. Thomas
1	MS 9915	N. M. Berry
1	MS 9915	M. L. Koszykowski
3	MS 9018	Central Technical Files, 8945-1
1	MS 0899	Technical Library, 9616
1	MS 9021	Classification Office, 8511 for Technical Library, MS 0899, 9616 DOE/OSTI via URL
1	MS 0188	D. Chavez, LDRD Office, 1011